JOURNAL OF NUMBER THEORY 7, 251–265 (1975)

p-adic Proofs of Congruences for the Bernoulli Numbers

WELLS JOHNSON

Department of Mathematics, Bowdoin College, Brunswick, Maine 04011

Communicated by H. Zassenhaus

Received July 25, 1974

Many of the classical theorems for the Bernoulli numbers, particularly those congruences needed in the study of irregular primes, follow easily from the existence of the $(p-1)$st roots of unity in the ring of p-adic integers. Proofs are given for the von Staudt–Clausen theorem, the theorem of J. C. Adams, the Friedmann–Tamarkine congruence, a theorem of Vandiver, special cases of the congruences of Voronoi, Kummer, and Carlitz, and the congruences of E. Lehmer.

1. INTRODUCTION AND NOTATION

Let p be a prime, and let U denote the group of units of the ring $\mathbf{Z}_p$ of p-adic integers. If V is the subgroup of U consisting of the $(p-1)$st roots of unity, then V, being a finite multiplicative subgroup of an integral domain, is cyclic and has order $p-1$. From the formula for the sum of a geometric series, it follows that, for $r \geqslant 1$,

$$\sum_{v \in V} v^r = \begin{cases} 0, & p-1 \nmid r \\ p-1, & p-1 \mid r. \end{cases} \tag{1}$$

In this paper we deduce many of the important classical theorems and congruences for the Bernoulli numbers directly from Eq. (1). The paper is reasonably self-contained and provides ready access to all of the fundamental congruences which have arisen in the study of irregular primes. The history of these congruences spans well over a century and the results are scattered throughout the literature. The presentation here not only gathers these results together, but it also shows how they can be proved from common, p-adic considerations.

In the next section we derive from Eq. (1) a fundamental equation for the Bernoulli numbers and use it to obtain immediately the von Staudt–Clausen theorem, theorems of J. C. Adams and Carlitz, the congruence of Friedmann and Tamarkine, and Kummer's congruence. In Section 3, we

show a connection between our theory and a conjecture of Iwasawa on the vanishing of the cyclotomic invariant μ_p. A proof of a special case of Voronoi's congruence and a theorem of Vandiver follows in Section 4. These congruences are equivalent and lead to other congruences which have been used to compute the irregular primes. In Section 5, we discuss the general congruences of Kummer and Carlitz, and in Section 6 we give proofs of the important congruences of E. Lehmer.

Any x in $\mathbf{Z}_p$ has the p-adic representation

$$x = \sum_{n=0}^{\infty} x_n p^n,$$

where the x_n are unique rational integers satisfying $0 \leqslant x_n < p$ for all $n \geqslant 0$. Whenever x is in $\mathbf{Z}_p$, we shall try to reserve the subscript notation x_n to denote the coefficient of p^n in the p-adic expansion of x.

For any rational integer a, $1 \leqslant a \leqslant p-1$, we let $v(a)$ denote the unique element of V satisfying $v(a) \equiv a \pmod{p}$. In particular, we always have, then, that $v(a)_0 = a$.

We let e_p denote the exponential p-adic valuation on $\mathbf{Z}_p$, or on its field of quotients, whenever this is appropriate.

For the sequence of Bernoulli numbers, B_r, we use the "even index" notation of [1]. The only fact that we shall need about the sequence of rational numbers B_r is the Euler–Maclaurin summation formula

$$(r+1) \sum_{a=1}^{n-1} a^r = \sum_{j=1}^{r} \binom{r+1}{j} B_{r+1-j}\, n^j + n^{r+1}, \tag{2a}$$

for $r, n \geqslant 1$. If we let $n = 1$ in Eq. (2a), we obtain the recursive definition of the sequence of Bernoulli numbers,

$$1 + \sum_{j=1}^{r} \binom{r+1}{j} B_{r+1-j} = 0, \qquad r \geqslant 1, \tag{2b}$$

which is equivalent to Eq. (2a). The usual proof that (2b) implies (2a) involves formal power series considerations, but the implication can also be proved by induction on $n \geqslant 1$.

2. Some Classical Results

We write the p-adic expansion for $v = v(a)$ in V as follows:

$$v = v(a) = a + t(a)\, p, \qquad t(a) = \sum_{n=1}^{\infty} v(a)_n\, p^{n-1} \in \mathbf{Z}_p. \tag{3}$$

Expanding the rth power of (3) and using Eq. (2a) with $n = p$, we obtain

$$\sum_{v \in V} v^r = \sum_{j=1}^{r} \binom{r}{j} p^j \left(\frac{B_{r+1-j}}{r+1-j} + \sum_{a=1}^{p-1} a^{r-j} t(a)^j \right) + \frac{p^{r+1}}{r+1}, \quad r \geqslant 1. \tag{4}$$

Equations (1) and (4) combine to give the fundamental formula

$$\beta_r + \sum_{a=1}^{p-1} a^{r-1} t(a) + \sum_{j=2}^{r} \frac{1}{r} \binom{r}{j} p^{j-1} \left(\frac{B_{r+1-j}}{r+1-j} + \sum_{a=1}^{p-1} a^{r-j} t(a)^j \right) + \frac{p^r}{(r+1)r} = 0, \tag{5}$$

where $r \geqslant 1$, and β_r is defined by

$$\beta_r = \begin{cases} B_r/r, & p-1 \nmid r \\ (B_r + p^{-1} - 1)/r, & p-1 \mid r. \end{cases}$$

We shall obtain results about the quotients β_r by examining Eq. (5) modulo various powers of the prime p.

LEMMA.

$$e_p\left(\frac{p^j}{j!}\right) > \frac{p-2}{p-1} j \quad \text{for} \quad j \geqslant 1.$$

Proof. Clearly, $e_p(p^j/j!) = j - e_p(j!)$. The Lemma follows from the well-known result that $(p-1)\, e_p(j!) = j - \sum_{n \geqslant 0} j_n$. If $j \geqslant 1$, then $\sum_{n \geqslant 0} j_n \geqslant 1$, giving us the inequality.

THEOREM 1. (a) *If $p \geqslant 3$, then $\beta_r \in \mathbf{Z}_p$ for all $r \geqslant 1$.*
(b) *If $p \geqslant 3$ and $p-1 \mid r$, then $pB_r + 1 \in p\mathbf{Z}_p$.*
(c) *$2B_r \in \mathbf{Z}_2$ for all $r \geqslant 1$, and $2B_r + 1 \in 2\mathbf{Z}_2$ for $r = 1$ and for r even.*

Proof. Part (b) follows from (a) by the definition of β_r. The proof is by induction on $r \geqslant 1$. The theorem is easily checked for $r = 1$, since $B_1 = -\frac{1}{2}$.

If $p \geqslant 3$, the Lemma implies that $e_p(p^{j-1}/j!) \geqslant 1$ for $j \geqslant 2$. The induction hypothesis then implies that each term indexed by j in Eq. (5) is in $\mathbf{Z}_p$. But, clearly, $p^r/(r+1)\, r \in \mathbf{Z}_p$ for $r \geqslant 2$, giving us (a).

If $p = 2$, then the Lemma merely gives us that $e_p(p^{j-1}/j!) \geqslant 0$. The induction hypothesis then implies that $2\beta_r \in \mathbf{Z}_2$ for all $r \geqslant 1$. But in this case, $p - 1 \mid r$ always, so that the definition of β_r gives us (c).

The corollaries below follow immediately from Theorem 1.

COROLLARY 1 (von Staudt–Clausen). *For $k \geqslant 1$, $B_{2k} + \sum_{p-1|2k} 1/p$ is a rational integer. In particular, the denominator of B_{2k} is exactly the product of those primes p such that $p - 1 \mid 2k$.*

COROLLARY 2 (J. C. Adams). *If $p - 1 \nmid 2k$ and $p^g \mid 2k$ for some $g \geqslant 1$, then p^g also divides the numerator of B_{2k}.*

COROLLARY 3 (Carlitz [2]). *If $p^g(p-1) \mid 2k$ for some $g \geqslant 1$, then p^g also divides the numerator of $B_{2k} + p^{-1} - 1$.*

If $p \geqslant 5$, then the Lemma implies that $e_p(p^{j-1}/j!) \geqslant 2$ for $j \geqslant 3$. Equation (5) then yields the congruence

$$\beta_r + \sum_{a=1}^{p-1} a^{r-1}t(a) + \frac{p}{2} B_{r-1} \equiv 0 \pmod{p}, \tag{6}$$

for $r \geqslant 2$ and $p \geqslant 5$.

The following theorem is a trivial consequence of the power series definition of the sequence B_r. We give another proof here, however, which depends only upon Eqs. (1) and (2b).

THEOREM 2. *For $k \geqslant 1$, $B_{2k+1} = 0$.*

Proof. We shall show that the sum in Eq. (6) vanishes (mod p) for $r = 2k + 1$ and all primes p such that $p - 1 \nmid 2k$. For these primes, $B_{r-1} \in \mathbf{Z}_p$ and $p \geqslant 5$, so that we may conclude from Eq. (6) that, for $k \geqslant 1$, $B_{2k+1} \equiv 0 \pmod{p}$ for infinitely many primes p. This will establish the result.

We note that $v(a)^p = v(a)$ implies that $a^p \equiv a + v(a)_1 p \pmod{p^2}$, so that $v(a)_1$ is completely determined by the conditions

$$v(a)_1 \equiv (a^p - a)/p \pmod{p}, \qquad 0 \leqslant v(a)_1 < p. \tag{7}$$

It follows that

$$v(a)_1 + v(p-a)_1 = p - 1, \qquad 1 \leqslant a \leqslant p - 1. \tag{8}$$

Clearly, $t(a) \equiv v(a)_1 \pmod{p}$, so that, letting $m = (p-1)/2$, we have by Eq. (8)

$$\sum_{a=1}^{p-1} a^{2k}t(a) \equiv \sum_{a=1}^{m} a^{2k}(v(a)_1 + v(p-a)_1) \equiv -\sum_{a=1}^{m} a^{2k} \pmod{p}.$$

But, since $p - 1 \nmid 2k$,

$$2 \sum_{a=1}^{m} a^{2k} \equiv \sum_{a=1}^{p-1} a^{2k} \equiv 0 \pmod{p},$$

so that the desired sum vanishes (mod p), concluding the proof.

Equation (7) implies that $t(a) \equiv aq_a \pmod{p}$, where q_a is the so-called Fermat quotient: $q_a = (a^{p-1} - 1)/p$. Letting $r = 2k$ in Eq. (6), we obtain the following theorem.

THEOREM 3. *If $p \geqslant 5$, then*

$$\beta_{2k} + \sum_{a=1}^{p-1} a^{2k} q_a \equiv 0 \pmod{p}, \qquad k \geqslant 1. \tag{9}$$

In the case $p - 1 \nmid 2k$, Eq. (9) goes back to Friedmann and Tamarkine [3], whose proof involved considerations of the greatest integer function $[x]$. If we let ω_p denote the so-called Wilson quotient, $((p-1)! + 1)/p$, we have the well-known relation $\sum_{a=1}^{p-1} q_a \equiv \omega_p \pmod{p}$. In the case $p - 1 \mid 2k$, Eq. (9) then yields the congruence $\beta_{2k} + \omega_p \equiv 0 \pmod{p}$, first proved by Carlitz [2]. E. Lehmer [12] used Kummer's congruence to prove Eq. (9) in the case $p - 1 \nmid 2k$. Since the approach here has been completely independent of Kummer's congruence, we may deduce it as an immediate corollary by the little theorem of Fermat.

COROLLARY (Kummer's Congruence). *If $p \geqslant 5$, then*

$$\beta_{2k} \equiv \beta_{2k+p-1} \pmod{p}.$$

In the case $p - 1 \nmid 2k$, the importance of this congruence is well known. Its use has been essential in all known proofs of the existence of infinitely many irregular primes.

We note in closing this section that, since $B_2 = \frac{1}{6}$, Eqs. (8) and (9) imply the interesting congruence

$$48 \sum_{a=1}^{m} av(a)_1 \equiv 1 \pmod{p}, \qquad p \geqslant 5.$$

This congruence can be used as a check in any actual computation of the numbers $v(1)_1 = 0$, $v(2)_1, \ldots, v(m)_1$. The present author [7, 22] has found good reason to compute these numbers for the irregular primes, and in fact he has done so for the irregular primes $p < 30000$.

3. The Cyclotomic Invariant μ_p of Iwasawa

We first prove a generalization of Eq. (9) in the case $p - 1 \nmid 2k$.

Theorem 4. *If* $p - 1 \nmid 2k$, *then*

$$\frac{B_{2k}}{2k} + u^{2k-1} \sum_{v \in V} (uv)_1 \, v^{2k-1} \equiv 0 \pmod{p} \tag{10}$$

for all p-adic units $u \in U$.

Proof. If $u = 1$, the result is included in Theorem 3. For general $u \in U$, we change the variable from v to $v(u_0)\, v$ in the sum for the case $u = 1$. Clearly, $(v(u_0)\, v)_0 \equiv u_0 v_0 \pmod{p}$, and a computation shows that $(v(u_0)\, v)_1 \equiv (uv)_1 + (v(u_0)_1 - u_1)\, v_0 \pmod{p}$. Hence,

$$\sum_{v \in V} v_1 v_0^{2k-1} \equiv u_0^{2k-1} \sum_{v \in V} (uv)_1 \, v_0^{2k-1} + u_0^{2k-1}(v(u_0)_1 - u_1) \sum_{v \in V} v_0^{2k} \pmod{p}.$$

But, since $p - 1 \nmid 2k$, the last sum vanishes (mod p), proving the theorem.

Iwasawa [4–6] has shown that the cyclotomic invariant $\mu_p > 0$ if and only if there exists an even index $2k$, $2 \leqslant 2k \leqslant p - 3$, such that

$$\sum_{v \in V} (uv)_n \, v^{2k-1} \equiv 0 \pmod{p} \tag{11}$$

for all p-adic units $u \in U$ and for all $n \geqslant 1$. Theorem 4 shows that the first of these conditions (i.e., the case $n = 1$) is merely equivalent to the condition that $B_{2k} \equiv 0 \pmod{p}$ for some $2k$, $2 \leqslant 2k \leqslant p - 3$ (in other words, that p be an irregular prime). No further restrictions may be derived from Eq. (11) with $n = 1$ by making various choices for the p-adic unit $u \in U$.

The present author [7, 22] has shown that $\mu_p = 0$ for all $p < 30000$ by deriving congruences from Eq. (11) for $n = 1, 2$ and then showing by an involved machine computation that these congruences fail to hold. Theorem 4 shows that the congruences derived from (11) with $n = 2$ were indeed needed to establish these results. It also implies that any proof of the conjecture that $\mu_p = 0$ for all primes p which relies on the conditions of (11) must in fact employ these congruences with values of $n \geqslant 2$.

4. Voronoi's Congruence and a Theorem of Vandiver

Some of the previous results of this paper are shown in [17] to follow from a fundamental congruence of Voronoi which dates back to 1889.

In this section, we use the formula of Theorem 4 to prove a special case of Voronoi's congruence. We then show that this result is equivalent to a theorem of Vandiver, which historically led to some of the fundamental congruences used to compute the irregular primes.

THEOREM 5 (Voronoi). *If $p - 1 \nmid 2k$ and b is a positive integer such that $p \nmid b$, then*

$$(b^{2k} - 1)\frac{B_{2k}}{2k} \equiv b^{2k-1} \sum_{a=1}^{p-1} \left[\frac{ba}{p}\right] a^{2k-1} \pmod{p}. \tag{12}$$

Proof. Since $p \nmid b$, we can consider b to be a p-adic unit. By Theorem 4, we obtain

$$\frac{B_{2k}}{2k} + b^{2k-1} \sum_{v \in V} (bv)_1 v^{2k-1} \equiv 0 \pmod{p}.$$

We multiply the case $b = 1$ by b^{2k} and subtract the above to obtain

$$(b^{2k} - 1)\frac{B_{2k}}{2k} \equiv b^{2k-1} \sum_{v \in V} ((bv)_1 - bv_1) v^{2k-1} \pmod{p}.$$

The result follows by noting that

$$(bv)_1 - bv_1 \equiv b_1 v_0 + \left[\frac{b_0 v_0}{p}\right] \equiv \left[\frac{bv_0}{p}\right] \pmod{p}.$$

For $p \equiv 3 \pmod 4$, we choose $b = 2$ and $2k = (p + 1)/2$ in Eq. (12) to obtain the congruence

$$\left(2 - \left(\frac{2}{p}\right)\right)\frac{B_{(p+1)/2}}{(p+1)/2} \equiv -\sum_{a=1}^{(p-1)/2} \left(\frac{a}{p}\right) \pmod{p},$$

where (a/p) denotes the Legendre symbol. The sum above cannot vanish, since it contains an odd number of terms, each of which is ± 1. Hence $B_{(p+1)/2} \not\equiv 0 \pmod p$ if $p \equiv 3 \pmod 4$, one of the few general results which seems to be known along these lines. It is well known (cf. [1, p. 346]), moreover, that the sum above is related to the class number $h(-p)$ of the quadratic field $\mathbf{Q}(\sqrt{-p})$. The congruence above proves that

$$2B_{(p+1)/2} \equiv -h(-p) \pmod{p},$$

a result first established by Friedmann and Tamarkine [3].

If we denote $[ba/p]$ by $j-1$ in Eq. (12), so that we have the inequality $(j-1)p < ba < jp$, then we obtain

$$(b^{2k}-1)\frac{B_{2k}}{2k} \equiv b^{2k-1}\sum_{j=1}^{b}(j-1)\sum_{(j-1)p<ba<jp} a^{2k-1} \pmod{p}.$$

Since $p-1 \nmid 2k-1$, then $\sum_{a=1}^{p-1} a^{2k-1} \equiv 0 \pmod{p}$, so that

$$(b^{2k}-1)\frac{B_{2k}}{2k} \equiv b^{2k-1}\sum_{j=1}^{b}(j-1-b)\sum_{(j-1)p<ba<jp} a^{2k-1} \pmod{p}.$$

This proves the following.

THEOREM 6 (Vandiver). *If $p-1 \nmid 2k$ and b is a positive integer such that $p \nmid b$, then*

$$(1-b^{2k})\frac{B_{2k}}{2k} \equiv b^{2k-1}\sum_{j=1}^{b}\sum_{a=1}^{[jp/b]} a^{2k-1} \pmod{p}. \tag{13}$$

Vandiver [18, 20] has given two other proofs of congruence (13). By choosing $b = 2, 3, 4$, and 6 in either (12) or (13) (which are equivalent), we can obtain the congruence

$$(4^{p-2k}+3^{p-2k}-6^{p-2k}-1)\frac{B_{2k}}{4k} \equiv \sum_{p/6<a<p/4} a^{2k-1} \pmod{p}.$$

A special case of this congruence dates back to Mirimanoff [13]. It was proved in general by Stafford and Vandiver [16], and it also appears as an exercise on Voronoi's congruence in [17]. The congruence has been important in the computational work on the Fermat Conjecture by Vandiver and others [7, 9, 11, 14–16, 19–22] over the past half-century. These various authors have used this congruence to compile tables of the irregular primes. They then proceeded to test the validity of Fermat's Last Theorem for all exponents less than various upper bounds by means of certain criteria developed by Vandiver.

5. The General Congruences of Kummer and Carlitz

If $x_1, x_2, x_3, \ldots$, is a sequence in any ring, we define the sequence of nth-order differences as follows:

$$\Delta^0 x_i = x_i, \qquad \Delta^1 x_i = x_{i+1} - x_i,$$

and

$$\Delta^n x_i = \Delta^1(\Delta^{n-1}x_i), \qquad \text{for} \quad n \geqslant 2.$$

The following elementary properties for these differences are well known:

(a) $\Delta^n x_i = \sum_{t=0}^{n} (-1)^{n-t} \binom{n}{t} x_{i+t}$;

(b) $\Delta^n(x_i y_i) = \sum_{t=0}^{n} \binom{n}{t} (\Delta^t x_i)(\Delta^{n-t} y_{i+t})$ (Leibniz' rule);

(c) if x_i is defined for all i by a polynomial in i of degree $< n$, then $\Delta^n x_i = 0$.

We now prove the following general congruences.

THEOREM 7. *Let the sequence of p-adic integers x_i be defined by $x_i = \beta_{2k+i(p-1)}$. Then, for $p \geqslant n + 3$ and $2k > n \geqslant 1$,*

$$\Delta^n x_i \equiv 0 \pmod{p^n}.$$

Proof. The proof is by induction on n, the case $n = 1$ having been proved already as the Corollary to Theorem 3. We assume $n \geqslant 2$ and use Eq. (5) with $r = 2k + i(p - 1)$. We show that the linear combination $\Delta^n y_i$ vanishes (mod p^n) for each term y_i in Eq. (5) other than the first.

For the second term, it's enough to let $y_i = (a^{p-1})^i$, where $1 \leqslant a \leqslant p - 1$. By (a) we have that

$$\Delta^n y_i = \sum_{t=0}^{n} (-1)^{n-t} \binom{n}{t} (a^{p-1})^{i+t} = (a^{p-1} - 1)^n a^{(p-1)i} \equiv 0 \pmod{p^n}.$$

We next deal with the terms indexed by j for $2 \leqslant j \leqslant n$, recalling that $n < 2k$. First, we consider terms of the form $(j!)^{-1} p^{j-1} p(i)\, z_i$, where $p(i)$ is a polynomial in i of degree $j - 1$ and $z_i = (a^{p-1})^i$ or $z_i = \beta_{2k+1-j+i(p-1)}$. Since $j \leqslant n < p$, it follows that $p \nmid j!$. Using (b) and (c), we see that

$$\Delta^n p(i)\, z_i = \sum_{t=0}^{j-1} \binom{n}{t} \Delta^t p(i)\, \Delta^{n-t} z_{i+t} .$$

It suffices to show that $\Delta^{n-t} z_{i+t} \equiv 0 \pmod{p^{n-j+1}}$ for $0 \leqslant t \leqslant j - 1$. In the case $z_i = (a^{p-1})^i$, the proof has been given above. For

$$z_i = \beta_{2k+1-j+i(p-1)} ,$$

the result follows by the induction hypothesis if $t \geqslant 1$. For $t = 0$, we simply note that the induction hypothesis also implies that

$$\Delta^n z_i = \Delta^{j-1}(\Delta^{n-j+1} z_i) \equiv 0 \pmod{p^{n-j+1}}.$$

Now, if $p - 1 \mid 2k + 1 - j$, we also must contend with expressions of the form $(j!)^{-1} p^{j-2} p(i)(p-1)$, where this time $p(i)$ is a polynomial in i of degree $j - 2$. The assumption $j \leqslant n$, however, implies that $\Delta^n p(i) = 0$ by (c).

We dispose of the remaining terms in Eq. (5) as follows. Since $p \geqslant n + 3$, the Lemma implies that

$$e_p(p^{j-1}/j!) \geqslant n + 1, \qquad \text{for} \quad j \geqslant n + 2$$

and

$$e_p(p^{j-1}/j!) \geqslant n, \qquad \text{for} \quad j = n + 1.$$

By Theorem 1, then, the only remaining term of Eq. (5) which might not vanish (mod p^n) is composed of terms of the form

$$\frac{1}{(2k)(2k-n)} \binom{2k}{n+1} p^{n-1}(pB_{2k-n}).$$

This poses a problem only if $p - 1 \mid 2k - n$. By Theorem 1, we have that $pB_{2k-n} \equiv -1 \pmod{p}$ in this case. Thus, in $\Delta^n y_i$, this term takes the form $p(i)(n+1)!^{-1} p^{n-1} \pmod{p^n}$, where $p(i)$ is a polynomial in i of degree $n - 1$. But then, by (c), $\Delta^n p(i) = 0$, concluding the proof.

Theorem 7 was first proved by Kummer [10] in the case $p - 1 \nmid 2k$, but without the restriction $p \geqslant n + 3$. An elementary proof based on Voronoi's congruence appears in Uspensky and Heaslet [17, p. 266]. In the case $p - 1 \mid 2k$, Theorem 7 was proved by Carlitz [2], but only under the restriction $2k \leqslant (p-1)(p-1-n-i)$. The approach here unifies these two results and also removes the restriction which Carlitz found necessary to impose upon the index $2k$.

Theorem 7 with $n = 2$ has been used by the present author [8, 22] to investigate the irregular prime divisors of the numerators of the Bernoulli numbers. In particular, computations have shown that, for all primes $p < 30000$ for which $B_{2k} \equiv 0 \pmod{p}$ for some index $2k$, $2 \leqslant 2k \leqslant p - 3$, it is never true that $\beta_{2k} \equiv \beta_{2k+p-1} \pmod{p^2}$. Iwasawa [4] has shown that the above congruences are necessary conditions for the cyclotomic invariant μ_p to be positive, and hence we have been able to conclude again that $\mu_p = 0$ for all primes $p < 30000$.

6. The Congruences of E. Lehmer

In this section, we first generalize Theorem 5, Voronoi's congruence, and then indicate how the generalization may be used to derive the important congruences of E. Lehmer [12]. The proof of Theorem 8 below follows along the lines of the more usual proof of Voronoi's congruence.

THEOREM 8. *If* $p - 1 \nmid 2k - 2$ *and* b *is a positive integer satisfying* $2 \leqslant b \leqslant p - 1$, *then*

$$(b^{2k} - 1)\frac{B_{2k}}{2k} \equiv b^{2k-1} \sum_{a=1}^{p-1} a^{2k-1} \left[\frac{ba}{p}\right] - \frac{2k-1}{2} pb^{2k-2} \sum_{a=1}^{p-1} a^{2k-2} \left[\frac{ba}{p}\right]^2 \pmod{p^2}. \quad (14)$$

Proof. We know that

$$\sum_{a=1}^{p-1} a^{2k} = \sum_{a=1}^{p-1} (v(a) - t(a)p)^{2k} = \sum_{v \in V} (v - t(v)p)^{2k},$$

where we let $t(v)$ denote $t(a)$ if $v = v(a)$. For $2 \leqslant b \leqslant p - 1$, we change the variable from v to $v(b)\, v$ in the last sum, obtaining

$$\sum_{a=1}^{p-1} a^{2k} = \sum_{v \in V} \left(bv_0 - \left[\frac{bv_0}{p}\right] p\right)^{2k}.$$

The assumption that $p - 1 \nmid 2k - 2$ implies that $p \geqslant 5$ and $2k \geqslant 4$. Suppose $e_p(2k) = g$. Using the Lemma and expanding the above, we obtain the congruence

$$(b^{2k} - 1) \sum_{a=1}^{p-1} a^{2k} \equiv 2kpb^{2k-1} \sum_{a=1}^{p-1} a^{2k-1} \left[\frac{ba}{p}\right] - \binom{2k}{2} p^2 b^{2k-2} \sum_{a=1}^{p-1} a^{2k-2} \left[\frac{ba}{p}\right]^2 \pmod{p^{g+3}}.$$

Similarly, we can deduce from Eq. (2a) that

$$\sum_{a=1}^{p-1} a^{2k} \equiv B_{2k} p \pmod{p^{g+3}}.$$

The result follows by combining the two congruences above, dividing by $2kp$, and noting that $e_p(2kp) = g + 1$.

By choosing $b = 2$, 3, 4, and 6 in Theorem 8, we obtain the following.

THEOREM 9 (E. Lehmer). *If* $p-1 \nmid 2k-2$, *then*

$$\text{(a)}\quad (2^{2k}-1)\frac{B_{2k}}{2k} \equiv \sum_{0<a<p/2} (p-2a)^{2k-1} \pmod{p^2},$$

$$\text{(b)}\quad (3^{2k}-1)\frac{B_{2k}}{4k} \equiv \sum_{0<a<p/3} (p-3a)^{2k-1} \pmod{p^2},$$

$$\text{(c)}\quad (2^{2k}-1)(2^{2k-1}+1)\frac{B_{2k}}{4k} \equiv \sum_{0<a<p/4} (p-4a)^{2k-1} \pmod{p^2},$$

$$\text{(d)}\quad (6^{2k-1}+3^{2k-1}+2^{2k-1}-1)\frac{B_{2k}}{4k} \equiv \sum_{0<a<p/6} (p-6a)^{2k-1} \pmod{p^2},$$

$$p \geqslant 7.$$

Proof. The proofs of (a)–(d) are similar so we provide the details of the proof for (b) only, as an example.

From Theorem 8 and with $b = 3$, we obtain

$$(3-3^{1-2k})\frac{B_{2k}}{2k} \equiv \sum_{p/3<a<2p/3} a^{2k-1} + 2\sum_{2p/3<a<p} a^{2k-1} - \frac{2k-1}{6}p\left(\sum_{p/3<a<2p/3} a^{2k-2} + 4\sum_{2p/3<a<p} a^{2k-2}\right) \pmod{p^2}.$$

By changing the variable from a to $p-a$, we see that

$$\sum_{p/3<a<2p/3} a^{2k-1} \equiv \frac{2k-1}{2}p\sum_{p/3<a<2p/3} a^{2k-2} \pmod{p^2},$$

and

$$\sum_{2p/3<a<p} a^{2k-1} \equiv -\sum_{0<a<p/3} a^{2k-1} + (2k-1)p\sum_{0<a<p/3} a^{2k-2} \pmod{p^2}.$$

Thus,

$$(3-3^{1-2k})\frac{B_{2k}}{2k} \equiv -2\sum_{0<a<p/3} a^{2k-1} + \frac{(2k-1)}{3}p\left(4\sum_{0<a<p/3} a^{2k-2} + \sum_{p/3<a<2p/3} a^{2k-2}\right) \pmod{p^2}.$$

But, since $p - 1 \nmid 2k - 2$, it follows that

$$2 \sum_{0<a<p/3} a^{2k-2} + \sum_{p/3<a<2p/3} a^{2k-2} \equiv \sum_{a=1}^{p-1} a^{2k-2} \equiv 0 \pmod{p}.$$

Hence,

$$(3^{2k} - 1)\frac{B_{2k}}{4k} \equiv -\sum_{0<a<p/3} (3a)^{2k-1} + (2k-1)p \sum_{0<a<p/3} (3a)^{2k-2}$$

$$\equiv \sum_{0<a<p/3} (p - 3a)^{2k-1} \pmod{p^2}.$$

The present author [8, 22] has used the congruences in Theorem 9 to compute various quotients $B_{2k}/2k \pmod{p^2}$ for the irregular primes $p < 30000$. Theorem 9 also has the following, very important corollary.

COROLLARY (E. Lehmer): *If* $p - 1 \nmid 2k - 2$, *then*

$$2^{2k-1}\frac{B_{2k}}{2k}p \equiv \frac{1}{2k}\sum_{0<a<p/2} (p - 2a)^{2k} \pmod{p^3}.$$

Proof. As we saw in the proof of Theorem 8, if $p - 1 \nmid 2k - 2$, then

$$\frac{1}{2k}\sum_{a=1}^{p-1} a^{2k} \equiv \frac{B_{2k}}{2k}p \pmod{p^3}.$$

By changing the variable from a to $p - a$ in the second half of the sum below, we obtain

$$\frac{1}{2k}\sum_{a=1}^{p-1} a^{2k} \equiv \frac{2}{2k}\sum_{0<a<p/2} a^{2k} - p\sum_{0<a<p/2} a^{2k-1}$$

$$+ \frac{2k-1}{2}p^2 \sum_{0<a<p/2} a^{2k-2} \pmod{p^3}.$$

Now the last term vanishes, since $p - 1 \nmid 2k - 2$ implies that

$$\sum_{0<a<p/2} a^{2k-2} \equiv 0 \pmod{p}.$$

Hence,

$$2^{2k-1}\frac{B_{2k}}{2k}p \equiv \frac{1}{2k}\sum_{0<a<p/2} (2a)^{2k} - p\sum_{0<a<p/2} (2a)^{2k-1}$$

$$\equiv \frac{1}{2k}\sum_{0<a<p/2} (2a)^{2k} + (2^{2k} - 1)\frac{B_{2k}}{2k}p \pmod{p^3},$$

by part (a) of Theorem 9. We then obtain

$$\frac{B_{2k}}{2k}p \equiv \frac{1}{2k}\sum_{a=1}^{p-1} a^{2k} \equiv \frac{1}{2k}\sum_{0<a<p/2} (2a)^{2k} + 2^{2k-1}\frac{B_{2k}}{2k}p \pmod{p^3},$$

which implies the statement of the Corollary.

This last congruence has proved to be of vital importance in the search for irregular primes. The congruence given at the end of Section 4 is useful for this search; one tests for the vanishing (mod p) of a sum containing only about $p/12$ terms. That congruence may be inconclusive, however, if the coefficient of $B_{2k}/4k$ also happens to vanish (mod p). In that event, the congruence above, taken (mod p^2), has provided a decisive test for irregularity.

References

1. Z. I. Borevič and I. R. Šafarevič, "Number Theory." Nauka Pub., Moscow, 1964; Academic Press, New York, 1966.
2. L. Carlitz, Some congruences for the Bernoulli numbers, *Amer. J. Math.* **75** (1953), 163–172.
3. A. Friedmann and J. Tamarkine, Quelques formules concernant la theorie de la fonction [x] et des nombres de Bernoulli, *J. Reine Angew. Math.* **135** (1909), 146–156.
4. K. Iwasawa, On some invariants of cyclotomic fields, *Amer. J. Math.* **80** (1958), 773–783; Erratum, *ibid.* **81** (1959), 280.
5. K. Iwasawa, A class number formula for cyclotomic fields, *Ann. Math.* **76** (1962), 171–179.
6. K. Iwasawa, On some modules in the theory of cyclotomic fields, *J. Math. Soc. Japan* **16** (1964), 42–82.
7. W. Johnson, On the vanishing of the Iwasawa invariant μ_p for $p < 8000$, *Math. Comp.* **27** (1973), 387–396.
8. W. Johnson, Irregular prime divisors of the Bernoulli numbers, *Math. Comp.* **28** (1974), 653–657.
9. V. V. Kobelev, Proof of Fermat's last theorem for all prime exponents less than 5500, *Sov. Math. Dokl.* **11** (1970), 188–190.
10. E. E. Kummer, Über eine allgemeine Eigenshaft der rational Entwickelungscoëfficienten einer bestimmten Gattung analytischer Functionen, *J. Reine Angew. Math.* **41** (1851), 368–372.
11. D. H. Lehmer, E. Lehmer, and H. S. Vandiver, An application of high-speed computing to Fermat's last theorem, *Proc. Nat. Acad. Sci. U.S.A.* **40** (1954), 25–33.
12. E. Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, *Ann. Math.* **39** (1938), 350–360.
13. D. Mirimanoff, L'équation indéterminée $x^l + y^l + z^l = 0$ et le critérium de Kummer, *J. Reine Angew. Math.* **128** (1905), 45–68.
14. J. L. Selfridge, C. A. Nicol, and H. S. Vandiver, Proof of Fermat's last theorem for all prime exponents less than 4002, *Proc. Nat. Acad. Sci. U.S.A.* **41** (1955), 970–973.

15. J. L. SELFRIDGE AND B. W. POLLACK, Fermat's last theorem is true for any exponent up to 25,000, *Not. Amer. Math. Soc.* **11** (1964), 97.
16. E. T. STAFFORD AND H. S. VANDIVER, Determination of some properly irregular cyclotomic fields, *Proc. Nat. Acad. Sci. U.S.A.* **16** (1930), 139–150.
17. J. USPENSKY AND M. HEASLET, "Elementary Number Theory." McGraw-Hill, New York, 1939.
18. H. S. VANDIVER, Symmetric functions formed by systems of elements of a finite algebra and their connection with Fermat's quotient and Bernoulli numbers, *Ann. Math.* **18** (1917), 105–114.
19. H. S. VANDIVER, Summary of results and proofs on Fermat's last theorem (Sixth paper), *Proc. Nat. Acad. Sci. U.S.A.* **17** (1931), 661–673.
20. H. S. VANDIVER, On Bernoulli's numbers and Fermat's last theorem, *Duke Math. J.* **3** (1937), 569–584.
21. H. S. VANDIVER, Examination of methods of attack on the second case of Fermat's last theorem, *Proc. Nat. Acad. Sci. U.S.A.* **40** (1954), 732–735.
22. W. JOHNSON, Irregular primes and cyclotomic invariants, *Math. Comp.* **29** (1975), 113–120.

Printed in Belgium